

PCT

REC'D 02 JUL 2001

WIPO

PCT

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70) 14

Applicant's or agent's file reference 402562WO	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP00/02617	International filing date (day/month/year) 23/03/2000	Priority date (day/month/year) 01/04/1999
International Patent Classification (IPC) or national classification and IPC H04L9/06		
Applicant KONINKLIJKE KPN N.V.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.


2. This REPORT consists of a total of 5 sheets, including this cover sheet.

- ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 9 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☐ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand  30/06/2000	Date of completion of this report  28.06.2001
Name and mailing address of the international preliminary examining authority:   European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer  Snell, T  Telephone No. +49 89 2399 8802



# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP00/02617

## I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

### Description, pages:

1-7 as received on 23/04/2001 with letter of 13/04/2001

### Claims, No.:

1-8 as received on 23/04/2001 with letter of 13/04/2001

### Drawings, sheets:

1/3-3/3 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP00/02617

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

*(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)*

6. Additional observations, if necessary:

### III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

☒ the entire international application.

☐ claims Nos. .

because:

☒ the said international application, or the said claims Nos. 1-8 relate to the following subject matter which does not require an international preliminary examination (*specify*):  
**see separate sheet**

☐ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. are so unclear that no meaningful opinion could be formed (*specify*):

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos. .

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the standard.

☐ the computer readable form has not been furnished or does not comply with the standard.

### VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

**see separate sheet**

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT - SEPARATE SHEET**

---

International application No. PCT/EP00/02617

**Cited documents**

- D1: EP-A-0 801 477 (TOKYO SHIBAURA ELECTRIC CO) 15 October 1997 (1997-10-15)  
D2: US-A-4 979 832 (RITTER TERRY F) 25 December 1990 (1990-12-25)  
D3: SCHUETT D ET AL: 'CRYPTOGRAPHIC PERMUTATIONS BASED ON BOOT DECOMPOSITIONS OF WALSH MATRICES' COMPUTER AIDED SYSTEMS THEORY. EUROCAST. SELECTION OF PAPERS FROM THE INTERNATIONAL WORKSHOP ON COMPUTER AIDED SYSTEMS THEORY, 1 February 1997 (1997-02-01), pages 580-590, XP002070120 BERLIN (DE)  
D4: EP-A-0 267 647 (PHILIPS NV) 18 May 1988 (1988-05-18)  
D5: MIYAGUCHI S: 'SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY' NTT REVIEW, vol. 6, no. 4, 1 July 1994 (1994-07-01), pages 85-90, XP000460342 TOKYO (JP)  
D6: US-A-4 157 454 (BECKER) 5 June 1979 (1979-06-05)

**Re Item III**

**Non-establishment of opinion with regard to novelty, inventive step and industrial applicability**

1. The method claimed in claims 1-8 is purely mathematical in character and thus relates to matter not requiring international preliminary examination under Rule 67.1(i) PCT (see PCT Guidelines IV-2.4(a)).
2. Although claim 1 now defines a "method for authentication of a string of input characters", authentication is in itself merely a mathematical problem. It only becomes technical when embedded in a real system, eg when the method is for authentication of a string of input characters transmitted from a sender to a receiver (cf decision T 208/84 (VICOM) of the Technical Board of Appeal of the European Patent Office, in particular point 5 of the reasons for the decision).
3. However, if the above objection had been overcome, or were to be overcome in a subsequent regional phase, it appears that the method of claim 1 would be novel and involve an inventive step over the prior art D1-D6 (Articles 33(1)-(3) PCT):

The essential features of the method according to the invention are that before encryption, the encryption function is modified under control of the input characters, and subsequently the input characters are encrypted by the modified function.

D1 discloses a modified function, but not under control of the input characters.

D2 discloses a modifying function as part of the encryption algorithm itself.

D3 discloses an r-round product cipher, whereby on each encryption round the key is changed, but not the encryption function.

D4 discloses a system in which an instruction command specifies the encryption function, but the encryption function is not chosen based on the input characters to be encrypted.

In D5, the encryption function is modified based on a key, but not on the input characters to be encrypted.

In D6, a key is modified based on the input characters, but the function is unchanged.

Although various combinations of documents could theoretically produce the invention, combining encryption functions is considered to be artificial and to involve an excessive use of hindsight given the large number of possible combinations and the lack of obvious compatibility between different algorithms.

### **Re Item VIII**

#### **Certain observations on the international application**

1. Claim 1 is not clear and does not define all the essential features of the invention, as although claim 1 claims a method for authentication, only an algorithm is defined, without any features being defined which would indicate how this algorithm is embedded in a method for authentication, eg there is no mention of the transmitted and received message (Article 6 PCT).

From the  
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

# PCT

## NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT (PCT Rule 71.1)

To:

KLEIN, Bart  
KONINKLIJKE KPN N.V.  
P.O. Box 95321  
NL-2509 CH Den Haag  
PAYS-BAS

Date of mailing  
(day/month/year) 28.06.2001

Applicant's or agent's file reference  
402562WO

### IMPORTANT NOTIFICATION

International application No.  
PCT/EP00/02617

International filing date (day/month/year)  
23/03/2000

Priority date (day/month/year)  
01/04/1999

Applicant  
KONINKLIJKE KPN N.V.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

#### 4. REMINDER

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/



European Patent Office  
D-80298 Munich  
Tel. +49 89 2399 - 0 Tx: 523656 epmu d  
Fax: +49 89 2399 - 4465

Authorized officer

Barrio Baranano, A

Tel. +49 89 2399-8621



# PCT

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT


(PCT Article 36 and Rule 70)

Applicant's or agent's file reference <b>402562WO</b>		<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. <b>PCT/EP00/02617</b>	International filing date (day/month/year) <b>23/03/2000</b>	Priority date (day/month/year) <b>01/04/1999</b>	
International Patent Classification (IPC) or national classification and IPC <b>H04L9/06</b>			
Applicant <b>KONINKLIJKE KPN N.V.</b>			

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 5 sheets, including this cover sheet.  
  
☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).  
  
 These annexes consist of a total of 9 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☐ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand  <b>30/06/2000</b>	Date of completion of this report  <b>28.06.2001</b>
Name and mailing address of the International preliminary examining authority:   <b>European Patent Office</b> <b>D-80298 Munich</b> <b>Tel. +49 89 2399 - 0 Tx: 523656 epmu d</b> <b>Fax: +49 89 2399 - 4465</b>	Authorized officer  <b>Snell, T</b>  Telephone No. <b>+49 89 2399 8802</b>



**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT**

International application No. PCT/EP00/02617

**I. Basis of the report**

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

**Description, pages:**

1-7 as received on 23/04/2001 with letter of 13/04/2001

**Claims, No.:**

1-8 as received on 23/04/2001 with letter of 13/04/2001

**Drawings, sheets:**

1/3-3/3 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).  
☐ the language of publication of the international application (under Rule 48.3(b)).  
☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.  
☐ filed together with the international application in computer readable form.  
☐ furnished subsequently to this Authority in written form.  
☐ furnished subsequently to this Authority in computer readable form.  
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.  
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:  
☐ the claims, Nos.:

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP00/02617

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

*(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)*

6. Additional observations, if necessary:

## III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

☒ the entire international application.

☐ claims Nos. .

because:

☒ the said international application, or the said claims Nos. 1-8 relate to the following subject matter which does not require an international preliminary examination (*specify*):  
**see separate sheet**

☐ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. are so unclear that no meaningful opinion could be formed (*specify*):

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos. .

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the standard.

☐ the computer readable form has not been furnished or does not comply with the standard.

## VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

**see separate sheet**

**Cited documents**

- D1: EP-A-0 801 477 (TOKYO SHIBAURA ELECTRIC CO) 15 October 1997 (1997-10-15)  
D2: US-A-4 979 832 (RITTER TERRY F) 25 December 1990 (1990-12-25)  
D3: SCHUETT D ET AL: 'CRYPTOGRAPHIC PERMUTATIONS BASED ON BOOT DECOMPOSITIONS OF WALSH MATRICES' COMPUTER AIDED SYSTEMS THEORY. EUROCAST. SELECTION OF PAPERS FROM THE INTERNATIONAL WORKSHOP ON COMPUTER AIDED SYSTEMS THEORY, 1 February 1997 (1997-02-01), pages 580-590, XP002070120 BERLIN (DE)  
D4: EP-A-0 267 647 (PHILIPS NV) 18 May 1988 (1988-05-18)  
D5: MIYAGUCHI S: 'SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY' NTT REVIEW, vol. 6, no. 4, 1 July 1994 (1994-07-01), pages 85-90, XP000460342 TOKYO (JP)  
D6: US-A-4 157 454 (BECKER) 5 June 1979 (1979-06-05)

**Re Item III**

**Non-establishment of opinion with regard to novelty, inventive step and industrial applicability**

1. The method claimed in claims 1-8 is purely mathematical in character and thus relates to matter not requiring international preliminary examination under Rule 67.1(i) PCT (see PCT Guidelines IV-2.4(a)).
2. Although claim 1 now defines a "method for authentication of a string of input characters", authentication is in itself merely a mathematical problem. It only becomes technical when embedded in a real system, eg when the method is for authentication of a string of input characters transmitted from a sender to a receiver (cf decision T 208/84 (VICOM) of the Technical Board of Appeal of the European Patent Office, in particular point 5 of the reasons for the decision).
3. However, if the above objection had been overcome, or were to be overcome in a subsequent regional phase, it appears that the method of claim 1 would be novel and involve an inventive step over the prior art D1-D6 (Articles 33(1)-(3) PCT):

The essential features of the method according to the invention are that before encryption, the encryption function is modified under control of the input characters, and subsequently the input characters are encrypted by the modified function.

D1 discloses a modified function, but not under control of the input characters.

D2 discloses a modifying function as part of the encryption algorithm itself.

D3 discloses an r-round product cipher, whereby on each encryption round the key is changed, but not the encryption function.

D4 discloses a system in which an instruction command specifies the encryption function, but the encryption function is not chosen based on the input characters to be encrypted.

In D5, the encryption function is modified based on a key, but not on the input characters to be encrypted.

In D6, a key is modified based on the input characters, but the function is unchanged.

Although various combinations of documents could theoretically produce the invention, combining encryption functions is considered to be artificial and to involve an excessive use of hindsight given the large number of possible combinations and the lack of obvious compatibility between different algorithms.

### **Re Item VIII**

#### **Certain observations on the international application**

1. Claim 1 is not clear and does not define all the essential features of the invention, as although claim 1 claims a method for authentication, only an algorithm is defined, without any features being defined which would indicate how this algorithm is embedded in a method for authentication, eg there is no mention of the transmitted and received message (Article 6 PCT).

Method for authentication of a string of input characters

The invention relates to a method according to the preamble of claim 1.

5 A method of said type is disclosed in EP-A-0399587. With the known method, the function ("algorithm") applied for enciphering consists of a non-linear function formed by a substitution box ("S box") generated as a function of the key. The document provides no further description of the way in which the substitution box is generated. For obtaining good  
10 statistical properties of the output of the substitution box with respect to variable import, a string of characters obtained by applying the substitution box are combined with just as long a string of statistically well-distributed characters. The string of characters obtained in this connection may be used for enciphering a string of input characters to be  
15 enciphered in an enciphered string of output characters. By applying a key-dependent substitution box instead of a permanent substitution box, the enciphering function is reinforced.

An objection to the known method is that, when there is substantially always used the same key, said reinforcement of the  
20 enciphering function in practice is appreciably annihilated. Such may occur, e.g., upon authentication when using a chip card, such as a calling card and a GSM card.

The object of the invention is to exclude the drawbacks of the known method. To this end, the invention provides a method as described in  
25 claim 1.

The sender of the enciphered string of output characters and the receiver of said series must both dispose of the same key and the string of input characters used for enciphering, at any rate the portion of the latter series used for modifying the function. As a result, the method is  
30 particularly suited for authentication, the receiver of an enciphered string of characters being capable of checking whether a sender having an identity suggested to the receiver has utilised a corresponding key, and in the event of a positive outcome of said check, the identity of the sender is ensured to the receiver.

35 The string of characters used for modifying the function are particularly variable and are, e.g., a challenge number generated per session, any (different) number, or a variable attribute of the sender, such as a balance kept up to date on a chip card.

If the non-linear function used for enciphering were an invertible  
40 function, the receiver of the enciphered string of characters may carry

out said check using the same function, the same key and the received string of characters as an input for the function. The result must be equal to the string of input characters used for enciphering.

Since the receiver may also carry out the check by executing the same operations as the ones carried out by the sender, the series received by the receiver having to be equal to the series generated by the receiver. In such case, it is not required that the function be an invertible function, as a result of which, in the event of the complexity remaining constant, there may be realised a stronger enciphering function which is more resistant against attacks.

The function applied to enciphering preferably is a non-linear function which may be formed by way of a substitution box or a cryptographic function, such as a function in which, depending on the input and the key, specific operations are carried out or not.

It is noted that EP0801477 discloses an encryption method in which an "internal state" is controlling an encryption function which, in each encryption round, modifies the encryption function. According to the present invention, the encryption function is modified only once, in an initial step, while always, after the initial modification, the same encryption function is used in every new encryption round. Contrary to that in the known method the encryption function is modified in every encryption round. Further, in the known method the encryption function is not modified on the basis of the input text. According to the present invention the input text forms an essential parameter in modifying the encryption function.

Next, it is noted that US4979832 discloses an enciphering method in which a pseudo-random input string is added to an encryption function. The pseudo-random string used in the encryption function also has to be available in the decryption process. In the known method the encryption function is dynamically (continuously) modified during the encryption processes. This is essential in the method according otherwise the system would be highly insecure. According to the present invention, however, there is only an initial modification of the encryption function, prior to the encryption process itself. Consequently, during the subsequent encryption process the encryption function is not changed any more. The known method is aimed at encryption/decryption. The method according to the invention is specifically designed for authentication and even can in practice not be used for encryption/decryption.

Further properties and advantages of the invention will become clear from the explanation following below of embodiments of the invention in conjunction with the enclosed drawings, in which:

FIG. 1 shows a diagram of a known enciphering function;

FIG. 2 shows a diagram of a first embodiment of the invention;

FIG. 3 shows a flow diagram for the operation of the embodiment according to FIG. 2; and

FIG. 4 shows a different embodiment of the invention.

By way of a block 1, FIG. 1 presents a known enciphering function (or encryption function). The enciphering function utilises one or more functions 2, also presented by blocks. Assuming a string of input characters IN 3 to be enciphered, the enciphering function using a secret key 4 determines an enciphered string of output characters EXIT 5. The known enciphering function DES [= Data Encryption Standard] operates according to said principle, eight non-linear functions being used which are formed by substitution boxes ("S boxes"). The invention is not limited, however, to the DES function; neither is it limited to using non-linear functions and substitution boxes for the functions.

FIG. 2 shows a diagram of an enciphering function 7 based on the enciphering function of FIG. 1 according to the invention. The functions are indicated by reference numeral 8. The functions 8 may be modified by applying an associated reference function 9 based on the string of input characters IN 3 or part thereof. The modification functions 9 need not be equal.

Below, the operation of the enciphering function of FIG. 2 will be explained with reference to the flow diagram of FIG. 3.

A modification function 9 modifies the function 8 based on a string of modification characters initially derived from the string of input characters IN 3 (block 11). Modifying the function 8 takes place in several steps, namely, the steps  $n=0$  to  $n=N_{\max}$  inclusive,  $N_{\max}$  being permitted to be permanent or also depending on, e.g., the series IN 3. That is why, at the start of the modification of the function 8, a step counter is reset (block 12). Subsequently, the function 8 is modified, based on the value of  $n$  and the modification series (block 13). Then the number of steps counted is incremented by 1 (block 14). Subsequently, it is checked whether the function 8 has already been modified the maximum number of times (block 15). When this condition is met, the modification of the function 8 is terminated; otherwise the string of modification characters are modified (step 16) and the function 8 is modified once again based on the new value of  $n$  and the modified string of modification characters (step

13). In Box I following below, an example is given for the operation of the enciphering function 7 shown in FIG. 2.

TABLE I

Step n	String of modification characters for $n > 0$ $x(2) :=$ $(x(0) + x(1)) \bmod 8$			From step $n=0$ , exchange $y(n \bmod 8)$ and $y(x(0))$							
	$x(0)$	$x(1)$	$x(2)$	i y(i)	0	1	2	3	4	5	6 7
0	5	2	3	4	0	5	7	6	3	1	2
1	2	3	7	4	5	0	7	6	3	1	2
2	3	7	5	4	5	7	0	6	3	1	2
3	7	5	2	4	5	7	2	6	3	1	0
4	5	2	4	4	5	7	2	3	6	1	0
5	2	4	7	4	5	6	2	3	7	1	0
6	4	7	6	4	5	6	2	1	7	3	0
7	7	6	3	4	5	6	2	1	7	3	0
8	6	3	5	1	5	6	2	4	7	3	0
9	3	5	1	1	2	6	5	4	7	3	0

It is assumed that the set of characters comprises eight characters, shown in the Table with the numerals 0 to 7 inclusive. It is further assumed that the function 8 is formed by a substitution box. Said box may be realised by a rewritable memory having eight memory locations containing addresses or sequential numbers  $1=0 \dots 7$ . The memory locations each comprise one of the characters, each character figuring only once in the memory locations. In Table I, the content of a memory location having address or sequential number  $i$  is indicated by  $y(i)$ . Initially, the memory locations for  $i=0 \dots 7$  contain the characters 3, 0, 5, 7, 6, 4, 1, 2, respectively. Said string of characters form an initial substitution box. A character of a string of characters to be enciphered is considered to be address or sequential number  $i$ , and is replaced by the character in the memory location having said address. According to the initial substitution box of Table I, e.g., 0 is therefore replaced by 3, 1 by 0, 2 by 5, ..., 7 by 2.

Before a string of characters to be enciphered are actually enciphered, according to the invention the initial substitution box is modified first. According to the example of Table I, modification takes place in ten steps (step  $n=0$  to  $n=N_{\max}$  inclusive). The modification takes

place depending on the characters of the string of characters to be enciphered, at any rate of several characters thereof. In Table I, the characters to be enciphered which are used for the modification of the substitution box are the characters 5, 2 and 3 indicated at step  $n=0$ .

5 Said characters are allotted to variables  $x(0)$ ,  $x(1)$  and  $x(2)$ , respectively.

During the first step with  $n=0$ , the character  $y(n)$ , i.e., the character 3 of memory location 0, is exchanged with the character  $y(x(0))$ , namely, character 4 of location  $x(0)=5$ . In Table I, for clarity's sake, 10 the exchanged characters of the substitution box of eight characters are underlined for each of the ten steps  $n=0, \dots, 9$ .

Subsequently, there is calculated an auxiliary variable  $h$ , which is equal to:

15  $h=(x(0)+x(1))$  modulo (the number of possible characters),  
or in the example  
 $h=(x(0)+x(1))$  modulo 8.

Subsequently, the characters of the string of modification characters  $x(0)$ ,  $x(1)$  and  $x(2)$  are replaced as follows (" $:=$ " means "becomes", i.e., an allotment).

20  $x(0):=x(1)$ ,  
 $x(1):=x(2)$ , and  
 $x(2):=h$ .

For each step, modifying characters based on the step number and the characters of the string of modification characters are repeated a 25 suitable number of times, in the example of Table I  $N_{\max}+1=10$  times. At the end of said modification function, the initial substitution box:

3, 0, 5, 7, 6, 4, 1, 2

has been replaced by a final substitution box:

1, 2, 6, 5, 4, 7, 3, 0.

30 Subsequently, the characters of an input series to be enciphered may, according to the order of the characters in the eventual substitution box, be replaced for providing an output string of enciphered characters. As a result, in the example the string of input characters 5, 2, 3 are replaced by 7, 6, 5, respectively. Said string of output characters are 35 used for possible further steps of the enciphering function.

FIG. 4 shows the diagram of an enciphering function 18 which differs from the enciphering function 5 of FIG. 2 in that the modification function 9 is replaced by a modification function 19. Just as the modification function 9, the modification function 19 depends on a number

of characters IN 3 to be enciphered, but in addition on a number of characters of the key 4.

Table II offers an example of the operation of the modification function 19.

5

TABLE II

Step n	String of modification characters for n>0 <u>x(2):=(x(0) + x(1))mod8</u>					From step n=0, exchange y(nmod8) and y(x(0))								
	x(0)	x(2)	x(4)			i	0	1	2	3	4	5	6	7
	x(1)	x(3)				y(i)	3	0	5	7	6	4	1	2
0	5	2	3	2	4		4	0	5	7	6	3	1	2
1	2	3	2	4	7		4	5	0	7	6	3	1	2
2	3	2	4	7	5		4	5	7	0	6	3	1	2
3	2	4	7	5	5		4	5	0	7	6	3	1	2
4	4	7	5	5	6		4	5	0	7	6	3	1	2
5	7	5	5	6	3		4	5	0	7	6	2	1	3
6	5	5	6	3	5		4	5	0	7	6	1	2	3
7	5	6	3	5	2		4	5	0	7	6	3	2	1
8	6	3	5	2	3		2	5	0	7	6	3	4	1
9	3	5	2	3	1		2	7	0	5	6	3	4	1

Table II differs from Table I only in that the string of modification characters  $x(0)$ ,  $x(1)$ ,  $x(2)$  are completed by  $x(3)$ ,  $x(4)$ . The characters  $x(3)$  and  $x(4)$  are derived from the key 4. In the example of Table II, the initial string of modification characters is 5, 2, 3, 2, 4. According to Table II, the eventual substitution box is:

2, 7, 0, 5, 6, 3, 4, 1.

The string of input characters IN 3 having the characters 5, 2, 3 is replaced, according to said eventual substitution box, by the enciphered string of output characters EXIT 20 having the characters 3, 0, 5.

The characters of the initial substitution box may be sorted at random for as long as both the sender of a string of enciphered characters UIT 5 and the receiver of the string of enciphered characters use the same initial substitution box. If it is possible to always meet said condition, the enciphering function may be reinforced by using, as an initial substitution box, a substitution box used during a preceding enciphering process, e.g., the most recently used eventual substitution

box. If there is a danger that said condition is not always met, it may be provided that the receiver of the string of enciphered characters 5 recalls several of such preceding substitution boxes and uses an older one thereof if deciphering the series received leads to a negative check  
5 result.

Since, both during enciphering a string of characters and during deciphering thereof, the keys used must be equal and knowledge must be available on the string of enciphered characters IN 3, the receiver of the enciphered series may carry out exactly the same operation, i.e.,  
10 enciphering, as the receiver has carried out, and compare the results to one another. In this event, a non-invertible function may be used for the function which, in the event of constant complexity, makes a stronger enciphering function possible.

The modification functions explained in conjunction with Tables I  
15 and II serve only as an example. For modifying the string of modification characters there may be applied, e.g., for each step, more than two and/or a different number of modulo additions, and the characters of the modification series may be rearranged in other ways instead of by way of simple shifting.

**This Page Blank (uspto)**

CLAIMS

1. Method for authentication of a string of input characters (3) by means of an enciphering function (2, 8) enabled for enciphering said string of input characters under control of a string of key characters (4), comprising the steps of:

- modifying, by application of a modification function, under control of a string of modification characters, said enciphering function;
- enciphering, by application of an enciphering function, under control of said string of key characters (4), said string of input characters,

CHARACTERISED in that

- said modification function (9, 19) is applied initially, prior to said application of the enciphering function and
- said initially applied modification function modifies the enciphering function (8) under control of modification characters which are derived from said string of input characters (3).

2. Method according to claim 1, characterised in that said modification characters are also derived from said string of key characters (4).

3. Method according to claim 1 or 2, characterised in that the modification function (9, 19) comprises the replacement of a character of the string of modification characters, by a replacement character obtained by an addition of two or more characters of the string of modification characters modulo the number of possible different characters.

4. Method according to any preceding claim, characterised in that the modification function (9, 19) comprises the modification of sequence numbers of two or more of the characters of the string of modification characters.

5. Method according to any preceding claim, characterised in that, for the modification of the function, there is used as an initial function the function which was used earlier for determining an earlier string of output characters (5, 20).

6. Method according to any preceding claim, characterised in that the function is a substitution function.

7. Method according to any of the claims 1 to 5 inclusive,  
5 characterised in that the function is a non-invertible function.

8. Method according to any of the preceding claims, characterised in that the function comprises a substitution box containing replacement characters for the characters of the string of input characters, and the  
10 modification function containing the exchange, depending on the string of modification characters, of two or more characters of the substitution box.

## PCT

## INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference <b>402562W0</b>	<b>FOR FURTHER ACTION</b> see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. <b>PCT/EP 00/ 02617</b>	International filing date (day/month/year) <b>23/03/2000</b>	(Earliest) Priority Date (day/month/year) <b>01/04/1999</b>
Applicant  <b>KONINKLIJKE KPN N.V.</b>		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

## 1. Basis of the report

- a. With regard to the language, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

- b. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international search was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ Certain claims were found unsearchable (See Box I).

3. ☐ Unity of Invention is lacking (see Box II).

## 4. With regard to the title,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

## 5. With regard to the abstract,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

## 6. The figure of the drawings to be published with the abstract is Figure No.

☒ as suggested by the applicant.

☐ because the applicant failed to suggest a figure.

☐ because this figure better characterizes the invention.

2

☐ None of the figures.

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 00/02617

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 801 477 A (TOKYO SHIBAURA ELECTRIC CO) 15 October 1997 (1997-10-15) abstract column 2, line 37 - line 50 column 4, line 7 - line 30 column 5, line 11 - line 31 column 9, line 8 - line 58 column 10, line 9 - line 26 column 11, line 1 - line 15	1,6,8
Y	US 4 979 832 A (RITTER TERRY F) 25 December 1990 (1990-12-25) column 5, line 50 - column 6, line 35 column 7, line 29 - line 40  -/-	1,6,8

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

5 June 2000

Date of mailing of the international search report

13/06/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Holper, G

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 00/02617

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SCHUETT D ET AL: "CRYPTOGRAPHIC PERMUTATIONS BASED ON BOOT DECOMPOSITIONS OF WALSH MATRICES" COMPUTER AIDED SYSTEMS THEORY. EUROCAST. SELECTION OF PAPERS FROM THE INTERNATIONAL WORKSHOP ON COMPUTER AIDED SYSTEMS THEORY, 1 February 1997 (1997-02-01), pages 580-590, XP002070120 BERLIN (DE)	1
A	EP 0 267 647 A (PHILIPS NV) 18 May 1988 (1988-05-18) column 2, last paragraph -column 3, line 12 column 3, line 52 -column 5, line 14	2
A	MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY" NTT REVIEW, vol. 6, no. 4, 1 July 1994 (1994-07-01), pages 85-90, XP000460342 TOKYO (JP) page 88, right-hand column, last paragraph -page 89, left-hand column, line 7	1
A	US 4 157 454 A (BECKER) 5 June 1979 (1979-06-05) abstract; figure 1; table 1	1,2,6

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 00/02617

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0801477	A	15-10-1997	AU 687306 B CA 2173688 A US 5740249 A AU 5063996 A	19-02-1998 10-10-1997 14-04-1998 16-10-1997
US 4979832	A	25-12-1990	NONE	
EP 0267647	A	18-05-1988	NL 8602847 A AU 611653 B AU 8095087 A CA 1291801 A JP 2628660 B JP 63135035 A US 4890324 A	01-06-1988 20-06-1991 12-05-1988 05-11-1991 09-07-1997 07-06-1988 26-12-1989
US 4157454	A	05-06-1979	DE 2658065 A CA 1101509 A FR 2375679 A GB 1577539 A JP 1200707 C JP 53094844 A JP 58032380 B	06-07-1978 19-05-1981 21-07-1978 22-10-1980 05-04-1984 19-08-1978 12-07-1983

From the INTERNATIONAL SEARCHING AUTHORITY

**PCT**NOTIFICATION OF TRANSMITTAL OF  
THE INTERNATIONAL SEARCH REPORT  
OR THE DECLARATION

(PCT Rule 44.1)

To:

KONINKLIJKE KPN N.V.  
Attn. KRUK, Wiggert Johan  
P.O. BOX 95321  
NL-2595 CH THE HAGUE  
NETHERLANDS

KPN GIE

Date of mailing  
(day/month/year)

13/06/2000

Applicant's or agent's file reference

402562W0

**FOR FURTHER ACTION**

See paragraphs 1 and 4 below

International application No.

PCT/EP 00/02617

International filing date  
(day/month/year)

23/03/2000

Applicant

KONINKLIJKE KPN N.V.

1. ☒ The applicant is hereby notified that the International Search Report has been established and is transmitted herewith.

**Filing of amendments and statement under Article 19:**

The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

**When?** The time limit for filing such amendments is normally 2 months from the date of transmittal of the International Search Report; however, for more details, see the notes on the accompanying sheet.

**Where?** Directly to the International Bureau of WIPO  
34, chemin des Colombettes  
1211 Geneva 20, Switzerland  
Facsimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no International Search Report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. ☐ With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:
- ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after 18 months from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.

Within 19 months from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within 20 months from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the International Searching Authority



European Patent Office, P.B. 5818 Patentlaan 2  
NL-2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Grace Casuga

## NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the PCT Applicant's Guide, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions respectively.

### INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

#### What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

#### When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

#### Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

#### How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

#### What documents must/may accompany the amendments?

##### Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

## NOTES TO FORM PCT/ISA/220 (continued)

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

- (i) the claim is unchanged;
- (ii) the claim is cancelled;
- (iii) the claim is new;
- (iv) the claim replaces one or more claims as filed;
- (v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:  
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."
2. [Where originally there were 15 claims and after amendment of all claims there are 11]:  
"Claims 1 to 15 replaced by amended claims 1 to 11."
3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:  
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or  
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."
4. [Where various kinds of amendments are made]:  
"Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

### "Statement under article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

**It must be in the language in which the international application is to be published.**

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

### Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the same time of filing the amendments with the International Bureau, also file a copy of such amendments with the International Preliminary Examining Authority (see Rule 62.2(a), first sentence).

### Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, where upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see Volume II of the PCT Applicant's Guide.

From the RECEIVING OFFICE

**PCT**

To:

Wiggert, Johan, Kruk  
KONINKLIJKE KPN N.V.  
P.O. Box 95321  
NL-2509 CH Den Haag  
PAYS-BAS

NOTIFICATION OF THE INTERNATIONAL  
APPLICATION NUMBER AND OF THE  
INTERNATIONAL FILING DATE

(PCT Rule 20.5(c))

Date of mailing  
(day/month/year)

04.04.2000

Applicant's or agent's file reference  
402562WO

## IMPORTANT NOTIFICATION

International application No.  
PCT/EP 00/02617International filing date (day/month/year)  
23/03/2000Priority date (day/month/year)  
01/04/1999Applicant  
KONINKLIJKE KPN N.V.

Title of the invention

1. The applicant is hereby notified that the international application has been accorded the international application number and the international filing date indicated above.
2. The applicant is further notified that the record copy of the international application was transmitted to the International Bureau on the above date of mailing.

3. ☐ Other:

\* The International Bureau monitors the transmittal of the record copy by the receiving Office and will notify the applicant (with Form PCT/IB/301) of its receipt. Should the record copy not have been received by the expiration of 14 months from the priority date, the International Bureau will notify the applicant (Rule 22.1(c)).

Name and mailing address of the receiving Office



European Patent Office, P.B. 5818 Patentlaan 2  
NL-2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

G. Koestel

IPEA/ EP

# PCT

## CHAPTER II

### DEMAND

under Article 31 of the Patent Cooperation Treaty:  
The undersigned requests that the international application specified below be the subject of international preliminary examination according to the Patent Cooperation Treaty and hereby elects all eligible States (except where otherwise indicated).

For International Preliminary Examining Authority use only	
Identification of IPEA	Date of receipt of DEMAND
<b>Box No. I IDENTIFICATION OF THE INTERNATIONAL APPLICATION</b>	
Applicant's or agent's file reference 402562W0	
International application No. PCT/EP00 /02617	International filing date (day/month/year) 23 MAR 2000(23/03/2000)
(Earliest) Priority date (day/month/year) 1 APR 1999(1/4/1999)	
Title of invention Method for enciphering a series of symbols applying a function and a key.	
<b>Box No. II APPLICANT(S)</b>	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)	
KONINKLIJKE KPN N.V. Stationsplein 7 9726 AE GRONINGEN The Netherlands	
Telephone No.: +31 70 3323678	
Facsimile No.: +31 70 3323840	
Teleprinter No.:	
State (that is, country) of nationality: NL	State (that is, country) of residence: NL
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)	
MULLER, Frank Meerkoetlaan 24 2623 NJ DELFT The Netherlands	
State (that is, country) of nationality: NL	State (that is, country) of residence: NL
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)	
PRINS, Sharon Christie Lesley Kleine Persterstraat 2-13 9711 KN GRONINGEN The Netherlands	
State (that is, country) of nationality: NL	State (that is, country) of residence: NL
<input checked="" type="checkbox"/> Further applicants are indicated on a continuation sheet.	

Continuation of Box No. II APPLICANT(S)

*If none of the following sub-boxes is used, this sheet should not be included in the demand.*Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

ROELOFSEN, Gerrit  
Rijndijk 60A  
2331 AH LEIDEN  
The Netherlands

State *(that is, country)* of nationality:

NL

State *(that is, country)* of residence:

NL

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*State *(that is, country)* of nationality:State *(that is, country)* of residence:Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*State *(that is, country)* of nationality:State *(that is, country)* of residence:Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*State *(that is, country)* of nationality:State *(that is, country)* of residence:☐

Further applicants are indicated on another continuation sheet.

**Box No. III AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE**

The following person is ☒ agent ☐ common representative  
 and ☐ has been appointed earlier and represents the applicant(s) also for international preliminary examination.  
☐ is hereby appointed and any earlier appointment of (an) agent(s)/common representative is hereby revoked.  
☒ is hereby appointed, specifically for the procedure before the International Preliminary Examining Authority, in addition to the agent(s)/common representative appointed earlier.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

Telephone No.:

+31 70 3323678

Facsimile No.:

+31 70 3323840

Teleprinter No.:

KLEIN, Bart  
 Koninklijke KPN N.V.  
 P.O. Box 95321  
 2509 CH The Hague  
 The Netherlands

☐ Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

**Box No. IV BASIS FOR INTERNATIONAL PRELIMINARY EXAMINATION**

**Statement concerning amendments:\***

1. The applicant wishes the international preliminary examination to start on the basis of:

☒ the international application as originally filed

the description ☒ as originally filed  
☐ as amended under Article 34

the claims ☒ as originally filed  
☐ as amended under Article 19 (together with any accompanying statement)  
☐ as amended under Article 34

the drawings ☒ as originally filed  
☐ as amended under Article 34

2. ☐ The applicant wishes any amendment to the claims under Article 19 to be considered as reversed.

3. ☐ The applicant wishes the start of the international preliminary examination to be postponed until the expiration of 20 months from the priority date unless the International Preliminary Examining Authority receives a copy of any amendments made under Article 19 or a notice from the applicant that he does not wish to make such amendments (Rule 69.1(d)). *(This check-box may be marked only where the time limit under Article 19 has not yet expired.)*

\* Where no check-box is marked, international preliminary examination will start on the basis of the international application as originally filed or, where a copy of amendments to the claims under Article 19 and/or amendments of the international application under Article 34 are received by the International Preliminary Examining Authority before it has begun to draw up a written opinion or the international preliminary examination report, as so amended.

**Language for the purposes of international preliminary examination: English**

☒ which is the language in which the international application was filed.

☐ which is the language of a translation furnished for the purposes of international search.

☐ which is the language of publication of the international application.

☐ which is the language of the translation (to be) furnished for the purposes of international preliminary examination.

**Box No. V ELECTION OF STATES**

The applicant hereby elects all eligible States *(that is, all States which have been designated and which are bound by Chapter II of the PCT)*

excluding the following States which the applicant wishes not to elect:

## Box No. VI CHECK LIST

The demand is accompanied by the following elements, in the language referred to in Box No. IV, for the purposes of international preliminary examination:

- |  |   |        |
|--|---|--------|
| 1. translation of international application                              | : | sheets |
| 2. amendments under Article 34   | : | sheets |
| 3. copy (or, where required, translation) of amendments under Article 19 | : | sheets |
| 4. copy (or, where required, translation) of statement under Article 19  | : | sheets |
| 5. letter  | : | sheets |
| 6. other (specify)   | : | sheets |

For International Preliminary Examining Authority use only

received	not received
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

The demand is also accompanied by the item(s) marked below:

- |   |   |
|---|---|
| 1. <input checked="" type="checkbox"/> fee calculation sheet  | 4. <input type="checkbox"/> statement explaining lack of signature                                  |
| 2. <input type="checkbox"/> separate signed power of attorney                                       | 5. <input type="checkbox"/> nucleotide and or amino acid sequence listing in computer readable form |
| 3. <input checked="" type="checkbox"/> copy of general power of attorney; reference number, if any: | 6. <input type="checkbox"/> other (specify):  |

## Box No. VII SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the demand).



Bart Klein  
The Professional Representative

For International Preliminary Examining Authority use only

- Date of actual receipt of DEMAND.
- Adjusted date of receipt of demand due to CORRECTIONS under Rule 60.1(b):
- ☐ The date of receipt of the demand is AFTER the expiration of 19 months from the priority date and item 4 or 5, below, does not apply. ☐ The applicant has been informed accordingly.
- ☐ The date of receipt of the demand is WITHIN the period of 19 months from the priority date as extended by virtue of Rule 80.5.
- ☐ Although the date of receipt of the demand is after the expiration of 19 months from the priority date, the delay in arrival is EXCUSED pursuant to Rule 82.

For International Bureau use only

Demand received from IPEA on:

# PCT

## CHAPTER II

### FEE CALCULATION SHEET

Annex to the Demand for international preliminary examination

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;"> International application No. <b>PCT/EP00/02617</b> </td> </tr> <tr> <td style="padding: 5px;"> Applicant's or agent's file reference <b>402562W0</b> </td> </tr> </table>	International application No. <b>PCT/EP00/02617</b>	Applicant's or agent's file reference <b>402562W0</b>	<p style="text-align: center;">For International Preliminary Examining Authority use only</p> <div style="border: 1px solid black; height: 100px; width: 100%;"></div>										
International application No. <b>PCT/EP00/02617</b>													
Applicant's or agent's file reference <b>402562W0</b>													
<p><b>Applicant</b></p> <p style="text-align: center;">Koninklijke KPN N.V.</p>													
<p><b>Calculation of prescribed fees</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;">1. Preliminary examination fee .....</td> <td style="width: 20%; border: 1px solid black; text-align: center;">EUR 1533</td> <td style="width: 20%; border: 1px solid black; text-align: center;">P</td> </tr> <tr> <td>2. Handling fee (Applicants from certain States are entitled to a reduction of 75% of the handling fee. Where the applicant is (or all applicants are) so entitled, the amount to be entered at H is 25% of the handling fee.) .....</td> <td style="border: 1px solid black; text-align: center;">EUR 147</td> <td style="border: 1px solid black; text-align: center;">H</td> </tr> <tr> <td>3. Total of prescribed fees Add the amounts entered at P and H and enter total in the TOTAL box .....</td> <td colspan="2" style="border: 1px solid black; text-align: center;">EUR 1680</td> </tr> <tr> <td></td> <td colspan="2" style="border: 1px solid black; text-align: center;">TOTAL</td> </tr> </table>		1. Preliminary examination fee .....	EUR 1533	P	2. Handling fee (Applicants from certain States are entitled to a reduction of 75% of the handling fee. Where the applicant is (or all applicants are) so entitled, the amount to be entered at H is 25% of the handling fee.) .....	EUR 147	H	3. Total of prescribed fees Add the amounts entered at P and H and enter total in the TOTAL box .....	EUR 1680			TOTAL	
1. Preliminary examination fee .....	EUR 1533	P											
2. Handling fee (Applicants from certain States are entitled to a reduction of 75% of the handling fee. Where the applicant is (or all applicants are) so entitled, the amount to be entered at H is 25% of the handling fee.) .....	EUR 147	H											
3. Total of prescribed fees Add the amounts entered at P and H and enter total in the TOTAL box .....	EUR 1680												
	TOTAL												
<p><b>Mode of Payment</b></p> <table style="width: 100%;"> <tr> <td><input checked="" type="checkbox"/> authorization to charge deposit account with the IPEA (see below)</td> <td><input type="checkbox"/> cash</td> </tr> <tr> <td><input type="checkbox"/> cheque</td> <td><input type="checkbox"/> revenue stamps</td> </tr> <tr> <td><input type="checkbox"/> postal money order</td> <td><input type="checkbox"/> coupons</td> </tr> <tr> <td><input type="checkbox"/> bank draft</td> <td><input type="checkbox"/> other (specify):</td> </tr> </table>		<input checked="" type="checkbox"/> authorization to charge deposit account with the IPEA (see below)	<input type="checkbox"/> cash	<input type="checkbox"/> cheque	<input type="checkbox"/> revenue stamps	<input type="checkbox"/> postal money order	<input type="checkbox"/> coupons	<input type="checkbox"/> bank draft	<input type="checkbox"/> other (specify):				
<input checked="" type="checkbox"/> authorization to charge deposit account with the IPEA (see below)	<input type="checkbox"/> cash												
<input type="checkbox"/> cheque	<input type="checkbox"/> revenue stamps												
<input type="checkbox"/> postal money order	<input type="checkbox"/> coupons												
<input type="checkbox"/> bank draft	<input type="checkbox"/> other (specify):												
<p><b>Deposit Account Authorization</b> (this mode of payment may not be available at all IPEAs)</p> <p>The IPEA/ <u>EP</u> <input checked="" type="checkbox"/> is hereby authorized to charge the total fees indicated above to my deposit account.</p> <p><input checked="" type="checkbox"/> (this check-box may be marked only if the conditions for deposit accounts of the IPEA so permit) is hereby authorized to charge any deficiency or credit any overpayment in the total fees indicated above to my deposit account.</p>													
<table style="width: 100%;"> <tr> <td style="width: 30%;">28090011</td> <td style="width: 30%; text-align: center;">26 June 2000</td> <td style="width: 40%; text-align: center;"> </td> </tr> <tr> <td>Deposit Account Number</td> <td>Date (day/month/year)</td> <td>Signature Klein, Bart</td> </tr> </table>		28090011	26 June 2000		Deposit Account Number	Date (day/month/year)	Signature Klein, Bart						
28090011	26 June 2000												
Deposit Account Number	Date (day/month/year)	Signature Klein, Bart											

21396 (rev.)

2 Ich (Wir) / I (We) / Je (Nous)

Koninklijke KPN N.V.  
Stationsplein 7  
9726 AE GRONINGEN  
The Netherlands

3 bevollmächtigt(n) hiermit / do hereby authorize / autorise (autorisons) par la présente

KLEIN, Bart (Professional Representative)

mailing address: Koninklijke KPN N.V.  
Intellectual Property Group  
P.O. Box 95321  
2509 CH THE HAGUE  
The Netherlands

4 mich (uns) in den durch das Europäische Patentübereinkommen geschaffenen Verfahren in allen meinen (unseren) Patentangelegenheiten zu vertreten  
alle Handlungen für mich (uns) vorzunehmen und Zahlungen für mich (uns) in Empfang zu nehmen.  
to represent me (us) in all proceedings established by the European Patent Convention and to act for me (us) in all patent transactions and to receive  
payments on my (our) behalf.  
à me (nous) représenter pour ce qui concerne toutes mes (nos) affaires de brevet dans toute procédure instituée par la Convention sur le brevet européen  
et, à ce titre, à agir en mon (notre) nom et à recevoir des paiements pour mon (notre) compte.

☒ Die Vollmacht gilt auch für Verfahren nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens.  
This authorisation shall also apply to the same extent to any proceedings established by the Patent Cooperation Treaty.  
Ce pouvoir s'applique également à toute procédure instituée par le Traité de coopération en matière de brevets.

☐ Weitere Vertreter sind auf einem gesonderten Blatt angegeben. / Additional representatives indicated on supplementary sheet.  
Les autres mandataires sont mentionnés sur une feuille supplémentaire.

5 ☒ Untervollmacht kann erteilt werden. / Sub-authorisation may be given. / Le pouvoir pourra être délégué.

6 ☒ Bitte die gelbe Kopie, ergänzt um die Nr. der allgemeinen Vollmacht, an den Vollmachtgeber zurücksenden.  
Please return the yellow copy, supplemented by the General Authorisation No., to the authoriser.  
Prière de renvoyer la copie jaune au mandant, munie du n° du pouvoir général.

Ort / Place / Lieu The Hague

Datum / Date September 01, 1998

Unterschrift(en) / Signature(s)

KLEIN, Bart (Professional Representative)

7 Das Formblatt muß vom (von den) Vollmachtgeber(n) (bei juristischen Personen vom Unterschriftsberechtigten) eigenhändig unterzeichnet sein. Nach der Unterschrift bitte die  
(die) Namen des (der) Unterzeichneten mit Schreibmaschine wiederholen (bei juristischen Personen die Stellung des Unterschriftsberechtigten innerhalb der Gesellschaft  
angeben).

The form must bear the personal signature(s) of the authorizer(s) (in the case of legal persons, that of the officer empowered to sign). After the signature, please type the name(s)  
of the signatory(ies) adding, in the case of legal persons, his (their) position within the company.

Le formulaire doit être signé de la propre main du (des) mandant(s) (dans le cas de personnes morales, de la personne ayant qualité pour signer). Veuillez ajouter à la machine  
après la signature, le (les) nom(s) du (des) signataire(s) en mentionnant, dans le cas de personnes morales, ses (leurs) fonctions au sein de la société.

PCT

## REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

PCT/EP 00/02617  
International Application No.23 MAR 2000 (23. 03. 2000)  
International Filing DateEUROPEAN PATENT OFFICE  
PCT INTERNATIONAL APPLICATION

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference  
(if desired) (12 characters maximum) 402562WO

## Box No. I TITLE OF INVENTION

Method for enciphering a series of symbols applying a function and a key.

## Box No. II APPLICANT

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

KONINKLIJKE KPN N.V.  
Stationsplein 7  
9726 AE GRONINGEN  
The Netherlands

☐ This person is also inventor.

Telephone No.

+31 70 3323678

Facsimile No.

+31 70 3323840

Teleprinter No.

State (that is, country) of nationality:

NL

State (that is, country) of residence:

NL

This person is applicant  
for the purposes of:☐all designated  
States☒all designated States except  
the United States of America☐the United States  
of America only☐the States indicated in  
the Supplemental Box

## Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

MULLER  
Frank  
Meerkoetlaan 24  
2623 NJ DELFT  
The Netherlands

This person is:

☐ applicant only☒ applicant and inventor☐ inventor only (If this check-box  
is marked, do not fill in below.)

State (that is, country) of nationality:

NL

State (that is, country) of residence:

NL

This person is applicant  
for the purposes of:☐all designated  
States☐all designated States except  
the United States of America☒the United States  
of America only☐the States indicated in  
the Supplemental Box☒ Further applicants and/or (further) inventors are indicated on a continuation sheet.

## Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:

☒

agent

☐

common representative

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)

Wiggert Johan KRUUK  
KONINKLIJKE KPN N.V.  
P.O. BOX 95321  
2509 CH THE HAGUE  
The Netherlands

Telephone No.

+31 70 3323678

Facsimile No.

+31 70 3323840

Teleprinter No.

☐ Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

## Continuation of Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

If none of the following sub-boxes is used, this sheet should not be included in the request.

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

PRINS  
Sharon Christie Lesley  
Kleine Pelsterstraat 2-13  
9711 KN GRONINGEN  
The Netherlands

This person is:

- ☐ applicant only  
☒ applicant and inventor  
☐ inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

NL

State (that is, country) of residence:

NL

This person is applicant for the purposes of:

☐ all designated States☐ all designated States except the United States of America☒ the United States of America only☐ the States indicated in the Supplemental Box

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

ROELOFSEN  
Gerrit  
Rijndijk 60-A  
2331 AH LEIDEN  
The Netherlands

This person is:

- ☐ applicant only  
☒ applicant and inventor  
☐ inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

NL

State (that is, country) of residence:

NL

This person is applicant for the purposes of:

☐ all designated States☐ all designated States except the United States of America☒ the United States of America only☐ the States indicated in the Supplemental Box

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

This person is:

- ☐ applicant only  
☐ applicant and inventor  
☐ inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

State (that is, country) of residence:

This person is applicant for the purposes of:

☐ all designated States☐ all designated States except the United States of America☐ the United States of America only☐ the States indicated in the Supplemental Box

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

This person is:

- ☐ applicant only  
☐ applicant and inventor  
☐ inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

State (that is, country) of residence:

This person is applicant for the purposes of:

☐ all designated States☐ all designated States except the United States of America☐ the United States of America only☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on another continuation sheet.

## Box No. V DESIGNATING STATES

The following designations are hereby made under Rule 4.9(a) (mark the applicable check-boxes; at least one must be marked):

## Regional Patent

- ☒ AP ARIPO Patent: GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, SD Sudan, SL Sierra Leone, SZ Swaziland, TZ United Republic of Tanzania, UG Uganda, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT
- ☒ EA Eurasian Patent: AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT
- ☒ EP European Patent: AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- ☒ OA OAPI Patent: BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT (if other kind of protection or treatment desired, specify on dotted line)

National Patent (if other kind of protection or treatment desired, specify on dotted line):

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> AE United Arab Emirates                  | <input checked="" type="checkbox"/> LR Liberia                                   |
| <input checked="" type="checkbox"/> AL Albania                               | <input checked="" type="checkbox"/> LS Lesotho                                   |
| <input checked="" type="checkbox"/> AM Armenia                               | <input checked="" type="checkbox"/> LT Lithuania                                 |
| <input checked="" type="checkbox"/> AT Austria                               | <input checked="" type="checkbox"/> LU Luxembourg                                |
| <input checked="" type="checkbox"/> AU Australia                             | <input checked="" type="checkbox"/> LV Latvia                                    |
| <input checked="" type="checkbox"/> AZ Azerbaijan                            | <input checked="" type="checkbox"/> MA Morocco                                   |
| <input checked="" type="checkbox"/> BA Bosnia and Herzegovina                | <input checked="" type="checkbox"/> MD Republic of Moldova                       |
| <input checked="" type="checkbox"/> BB Barbados                              | <input checked="" type="checkbox"/> MG Madagascar                                |
| <input checked="" type="checkbox"/> BG Bulgaria                              | <input checked="" type="checkbox"/> MK The former Yugoslav Republic of Macedonia |
| <input checked="" type="checkbox"/> BR Brazil                                |  |
| <input checked="" type="checkbox"/> BY Belarus                               | <input checked="" type="checkbox"/> MN Mongolia                                  |
| <input checked="" type="checkbox"/> CA Canada                                | <input checked="" type="checkbox"/> MW Malawi                                    |
| <input checked="" type="checkbox"/> CH and LI Switzerland and Liechtenstein  | <input checked="" type="checkbox"/> MX Mexico                                    |
| <input checked="" type="checkbox"/> CN China                                 | <input checked="" type="checkbox"/> NO Norway                                    |
| <input checked="" type="checkbox"/> CR Costa Rica                            | <input checked="" type="checkbox"/> NZ New Zealand                               |
| <input checked="" type="checkbox"/> CU Cuba                                  | <input checked="" type="checkbox"/> PL Poland                                    |
| <input checked="" type="checkbox"/> CZ Czech Republic                        | <input checked="" type="checkbox"/> PT Portugal                                  |
| <input checked="" type="checkbox"/> DE Germany                               | <input checked="" type="checkbox"/> RO Romania                                   |
| <input checked="" type="checkbox"/> DK Denmark                               | <input checked="" type="checkbox"/> RU Russian Federation                        |
| <input checked="" type="checkbox"/> DM Dominica                              | <input checked="" type="checkbox"/> SD Sudan                                     |
| <input checked="" type="checkbox"/> EE Estonia                               | <input checked="" type="checkbox"/> SE Sweden                                    |
| <input checked="" type="checkbox"/> ES Spain                                 | <input checked="" type="checkbox"/> SG Singapore                                 |
| <input checked="" type="checkbox"/> FI Finland                               | <input checked="" type="checkbox"/> SI Slovenia                                  |
| <input checked="" type="checkbox"/> GB United Kingdom                        | <input checked="" type="checkbox"/> SK Slovakia                                  |
| <input checked="" type="checkbox"/> GD Grenada                               | <input checked="" type="checkbox"/> SL Sierra Leone                              |
| <input checked="" type="checkbox"/> GE Georgia                               | <input checked="" type="checkbox"/> TJ Tajikistan                                |
| <input checked="" type="checkbox"/> GH Ghana                                 | <input checked="" type="checkbox"/> TM Turkmenistan                              |
| <input checked="" type="checkbox"/> GM Gambia                                | <input checked="" type="checkbox"/> TR Turkey                                    |
| <input checked="" type="checkbox"/> HR Croatia                               | <input checked="" type="checkbox"/> TT Trinidad and Tobago                       |
| <input checked="" type="checkbox"/> HU Hungary                               | <input checked="" type="checkbox"/> TZ United Republic of Tanzania               |
| <input checked="" type="checkbox"/> ID Indonesia                             | <input checked="" type="checkbox"/> UA Ukraine                                   |
| <input checked="" type="checkbox"/> IL Israel                                | <input checked="" type="checkbox"/> UG Uganda                                    |
| <input checked="" type="checkbox"/> IN India                                 | <input checked="" type="checkbox"/> US United States of America                  |
| <input checked="" type="checkbox"/> IS Iceland                               |  |
| <input checked="" type="checkbox"/> JP Japan                                 | <input checked="" type="checkbox"/> UZ Uzbekistan                                |
| <input checked="" type="checkbox"/> KE Kenya                                 | <input checked="" type="checkbox"/> VN Viet Nam                                  |
| <input checked="" type="checkbox"/> KG Kyrgyzstan                            | <input checked="" type="checkbox"/> YU Yugoslavia                                |
| <input checked="" type="checkbox"/> KP Democratic People's Republic of Korea | <input checked="" type="checkbox"/> ZA South Africa                              |
|  | <input checked="" type="checkbox"/> ZW Zimbabwe                                  |
| <input checked="" type="checkbox"/> KR Republic of Korea                     |  |
| <input checked="" type="checkbox"/> KZ Kazakhstan                            |  |
| <input checked="" type="checkbox"/> LC Saint Lucia                           |  |
| <input checked="" type="checkbox"/> LK Sri Lanka                             |  |

Check-boxes reserved for designating States which have become party to the PCT after issuance of this sheet:

- ☐ .....
- ☐ .....

**Precautionary Designation Statement:** In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. (Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)

<b>Box No. VI PRIORITY</b>		<input type="checkbox"/> Further priority claims are indicated in the Supplemental Box.		
Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is:		
		national application: country	regional application: regional Office	international application: receiving Office
item (1) (01.04.99) 1 APR 1999	1011719	NL		
item (2)				
item (3)				

☐ The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) (only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office) identified above as item(s):

\* Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.

### Box No. VII INTERNATIONAL SEARCHING AUTHORITY

**Choice of International Searching Authority (ISA)**  
(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):

ISA/ EP

**Request to use results of earlier search; reference to that search (if an earlier search has been carried out by or requested from the International Searching Authority):**

Date (day/month/year)

Number

Country (or regional Office)

30 AUG 1999

SN33093NL

NL

### Box No. VIII CHECK LIST: LANGUAGE OF FILING

This international application contains the following number of sheets:

request : 7  
description (excluding sequence listing part) : 6  
claims : 2  
abstract : 1  
drawings : 3  
sequence listing part of description : 1

Total number of sheets : 19

This international application is accompanied by the item(s) marked below:

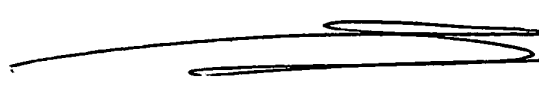
1. ☒ fee calculation sheet
2. ☒ separate signed power of attorney
3. ☒ copy of general power of attorney; reference number, if any:
4. ☐ statement explaining lack of signature
5. ☐ priority document(s) identified in Box No. VI as item(s):
6. ☐ translation of international application into (language):
7. ☐ separate indications concerning deposited microorganism or other biological material
8. ☐ nucleotide and/or amino acid sequence listing in computer readable form
9. ☒ other (specify): search report

Figure of the drawings which should accompany the abstract: 2

Language of filing of the international application: English

### Box No. IX SIGNATURE OF APPLICANT OR AGENT

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).



KRUK, Wiggert Johan

For receiving Office use only		2. Drawings: <input checked="" type="checkbox"/> received:  <input type="checkbox"/> not received:
1. Date of actual receipt of the purported international application:	(23. 03. 2000) 23 MAR 2000	
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:		
4. Date of timely receipt of the required corrections under PCT Article 11(2):		
5. International Searching Authority (if two or more are competent): ISA/	6. <input type="checkbox"/> Transmittal of search copy delayed until search fee is paid.	

Date of receipt of the record copy by the International Bureau:

For International Bureau use only

## Supplemental Box

If Supplemental Box is not used, this sheet should not be included in the request.

1. If, in any of the Boxes, the space is insufficient to furnish all the information: in such case, write "Continuation of Box No. ..." [indicate the number of the Box] and furnish the information in the same manner as required according to the captions of the Box in which the space was insufficient, in particular:
  - (i) if more than two persons are involved as applicants and/or inventors and no "continuation sheet" is available: in such case, write "Continuation of Box No. III" and indicate for each additional person the same type of information as required in Box No. III. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below;
  - (ii) if, in Box No. II or in any of the sub-boxes of Box No. III, the indication "the States indicated in the Supplemental Box" is checked: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the applicant(s) involved and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is applicant;
  - (iii) if, in Box No. II or in any of the sub-boxes of Box No. III, the inventor or the inventor/applicant is not inventor for the purposes of all designated States or for the purposes of the United States of America: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the inventor(s) and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is inventor;
  - (iv) if, in addition to the agent(s) indicated in Box No. IV, there are further agents: in such case, write "Continuation of Box No. IV" and indicate for each further agent the same type of information as required in Box No. IV;
  - (v) if, in Box No. V, the name of any State (or OAPI) is accompanied by the indication "patent of addition," or "certificate of addition," or if, in Box No. V, the name of the United States of America is accompanied by an indication "continuation" or "continuation-in-part": in such case, write "Continuation of Box No. V" and the name of each State involved (or OAPI), and after the name of each such State (or OAPI), the number of the parent title or parent application and the date of grant of the parent title or filing of the parent application;
  - (vi) if, in Box No. VI, there are more than three earlier applications whose priority is claimed: in such case, write "Continuation of Box No. VI" and indicate for each additional earlier application the same type of information as required in Box No. VI;
  - (vii) if, in Box No. VI, the earlier application is an ARIPO application: in such case, write "Continuation of Box No. VI", specify the number of the item corresponding to that earlier application and indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed.
2. If, with regard to the precautionary designation statement contained in Box No. V, the applicant wishes to exclude any State(s) from the scope of that statement: in such case, write "Designation(s) excluded from precautionary designation statement" and indicate the name or two-letter code of each State so excluded.
3. If the applicant claims, in respect of any designated Office, the benefits of provisions of the national law concerning non-prejudicial disclosures or exceptions to lack of novelty: in such case, write "Statement concerning non-prejudicial disclosures or exceptions to lack of novelty" and furnish that statement below.



MULLER  
Frank

## Supplemental Box

If the Supplemental Box is not used, this sheet should not be included in the request.

1. If, in any of the Boxes, the space is insufficient to furnish all the information: in such case, write "Continuation of Box No. ..." [indicate the number of the Box] and furnish the information in the same manner as required according to the captions of the Box in which the space was insufficient, in particular:
  - (i) if more than two persons are involved as applicants and/or inventors and no "continuation sheet" is available: in such case, write "Continuation of Box No. III" and indicate for each additional person the same type of information as required in Box No. III. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below;
  - (ii) if, in Box No. II or in any of the sub-boxes of Box No. III, the indication "the States indicated in the Supplemental Box" is checked: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the applicant(s) involved and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is applicant;
  - (iii) if, in Box No. II or in any of the sub-boxes of Box No. III, the inventor or the inventor/applicant is not inventor for the purposes of all designated States or for the purposes of the United States of America: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the inventor(s) and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is inventor;
  - (iv) if, in addition to the agent(s) indicated in Box No. IV, there are further agents: in such case, write "Continuation of Box No. IV" and indicate for each further agent the same type of information as required in Box No. IV;
  - (v) if, in Box No. V, the name of any State (or OAPI) is accompanied by the indication "patent of addition," or "certificate of addition," or if, in Box No. V, the name of the United States of America is accompanied by an indication "continuation" or "continuation-in-part": in such case, write "Continuation of Box No. V" and the name of each State involved (or OAPI), and after the name of each such State (or OAPI), the number of the parent title or parent application and the date of grant of the parent title or filing of the parent application;
  - (vi) if, in Box No. VI, there are more than three earlier applications whose priority is claimed: in such case, write "Continuation of Box No. VI" and indicate for each additional earlier application the same type of information as required in Box No. VI;
  - (vii) if, in Box No. VI, the earlier application is an ARIPO application: in such case, write "Continuation of Box No. VI", specify the number of the item corresponding to that earlier application and indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed.
2. If, with regard to the precautionary designation statement contained in Box No. V, the applicant wishes to exclude any State(s) from the scope of that statement: in such case, write "Designation(s) excluded from precautionary designation statement" and indicate the name or two-letter code of each State so excluded.
3. If the applicant claims, in respect of any designated Office, the benefits of provisions of the national law concerning non-prejudicial disclosures or exceptions to lack of novelty: in such case, write "Statement concerning non-prejudicial disclosures or exceptions to lack of novelty" and furnish that statement below.

PRINS

Sharon Christie Lesley



## Supplemental Box

If Supplemental Box is not used, this sheet should not be included in the request.

1. If, in any of the Boxes, the space is insufficient to furnish all the information: in such case, write "Continuation of Box No. ..." [indicate the number of the Box] and furnish the information in the same manner as required according to the captions of the Box in which the space was insufficient, in particular:
  - (i) if more than two persons are involved as applicants and/or inventors and no "continuation sheet" is available: in such case, write "Continuation of Box No. III" and indicate for each additional person the same type of information as required in Box No. III. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below;
  - (ii) if, in Box No. II or in any of the sub-boxes of Box No. III, the indication "the States indicated in the Supplemental Box" is checked: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the applicant(s) involved and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is applicant;
  - (iii) if, in Box No. II or in any of the sub-boxes of Box No. III, the inventor or the inventor/applicant is not inventor for the purposes of all designated States or for the purposes of the United States of America: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the inventor(s) and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is inventor;
  - (iv) if, in addition to the agent(s) indicated in Box No. IV, there are further agents: in such case, write "Continuation of Box No. IV" and indicate for each further agent the same type of information as required in Box No. IV;
  - (v) if, in Box No. V, the name of any State (or OAPI) is accompanied by the indication "patent of addition," or "certificate of addition," or if, in Box No. V, the name of the United States of America is accompanied by an indication "continuation" or "continuation-in-part": in such case, write "Continuation of Box No. V" and the name of each State involved (or OAPI), and after the name of each such State (or OAPI), the number of the parent title or parent application and the date of grant of the parent title or filing of the parent application;
  - (vi) if, in Box No. VI, there are more than three earlier applications whose priority is claimed: in such case, write "Continuation of Box No. VI" and indicate for each additional earlier application the same type of information as required in Box No. VI;
  - (vii) if, in Box No. VI, the earlier application is an ARIPO application: in such case, write "Continuation of Box No. VI", specify the number of the item corresponding to that earlier application and indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed.
2. If, with regard to the precautionary designation statement contained in Box No. V, the applicant wishes to exclude any State(s) from the scope of that statement: in such case, write "Designation(s) excluded from precautionary designation statement" and indicate the name or two-letter code of each State so excluded.
3. If the applicant claims, in respect of any designated Office, the benefits of provisions of the national law concerning non-prejudicial disclosures or exceptions to lack of novelty: in such case, write "Statement concerning non-prejudicial disclosures or exceptions to lack of novelty" and furnish that statement below.

ROELOFSEN  
Gerrit